Classifying Data At U-M

Svetla Sytch and Asmat Noori

ITS Information Assurance

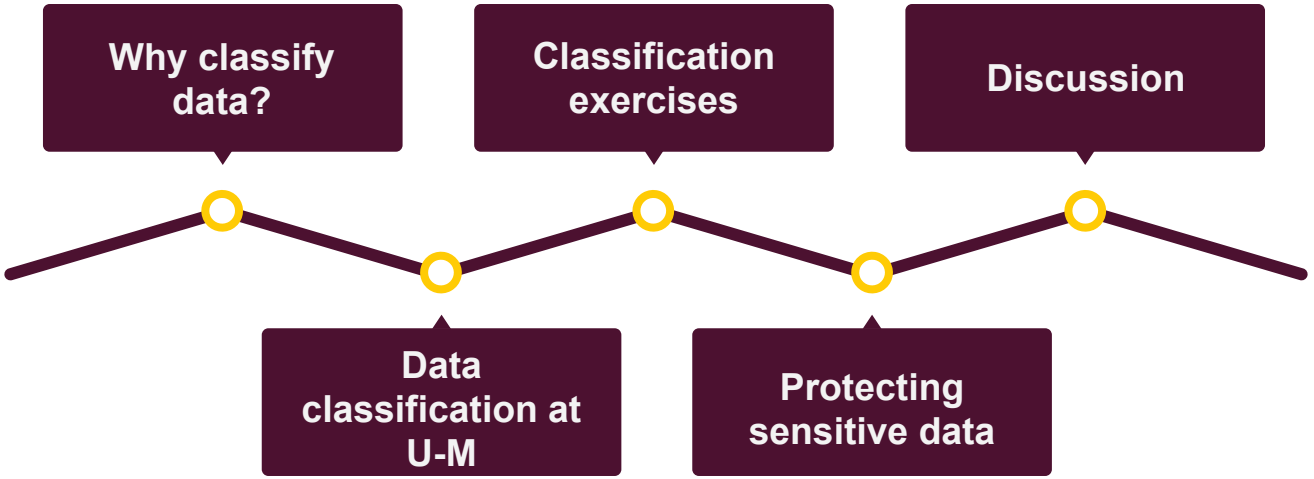
INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

SUMIT_2020 Reimagined

Security and Compliance at U-M

- Do not conflate security and compliance
- Security and compliance are a shared responsibility
- Alignment vs. compliance: do the right thing to the best of your ability
- Using common sense
- It’s a never-ending journey
- Information Assurance is a partner and a resource to you

Today's Journey



Why Classify Data

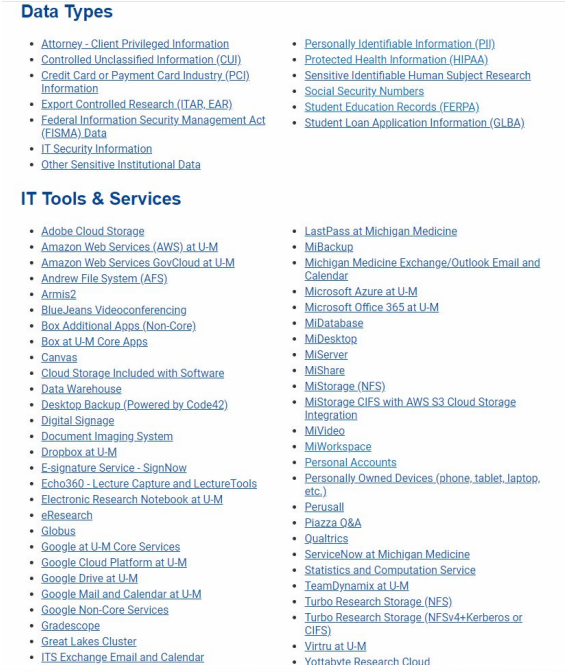
Data classification helps:

- ➔ Meet legal, regulatory, academic, financial, and operational requirements
- ➔ Determine minimum security requirements
- ➔ Take a risk-based approach to data protection
- ➔ Balance protection of data confidentiality and integrity with the need for collaboration and sharing of knowledge

U-M Data Classification Levels

Restricted	• Disclosure **could cause severe harm** to individuals and/or the university, including exposure to criminal and civil liability. • Has the most stringent legal or regulatory requirements and **requires the most prescriptive security controls**.	Credit card numbers (PCI); FISMA
High	• Disclosure **could cause significant harm** to individuals and/or the university, including exposure to criminal and civil liability. • Usually **subject to legal and regulatory requirements** due to data that are individually identifiable, highly sensitive, and/or confidential.	HIPAA, CUI, ITAR, SSN, GLBA, etc.
Moderate	• Disclosure **could cause limited harm** to individuals and/or the university with some risk of civil liability. • **May be subject to contractual agreements or regulatory compliance**, or is individually identifiable, confidential, and/or proprietary.	Building plans, contracts, employee records, FERPA, UMID with names, etc.
Low	• Encompasses public information and data for which disclosure **poses little to no risk** to individuals and/or the university. • **Anyone** regardless of institutional affiliation **can access** without limitation.	Directory information, public websites, research proposals, course catalogs, UMID w/o names, etc.

The U-M Sensitive Data Guide

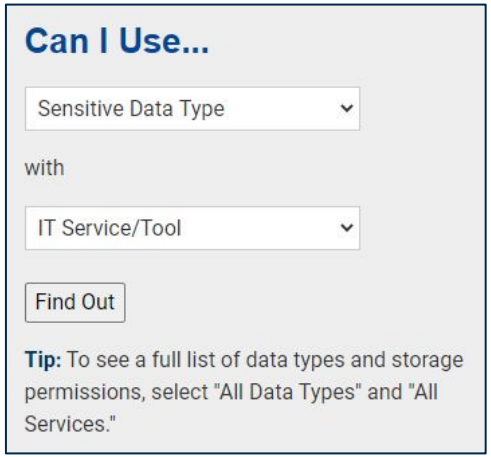


Data Types

- Attorney - Client Privileged Information
- Controlled Unclassified Information (CUI)
- Credit Card or Payment Card Industry (PCI) Information
- Export Controlled Research (ITAR, EAR)
- Federal Information Security Management Act (FISMA) Data
- IT Security Information
- Other Sensitive Institutional Data
- Personally Identifiable Information (PII)
- Protected Health Information (HIPAA)
- Sensitive Identifiable Human Subject Research
- Social Security Numbers
- Student Education Records (FERPA)
- Student Loan Application Information (GLBA)

IT Tools & Services

- Adobe Cloud Storage
- Amazon Web Services (AWS) at U-M
- Amazon Web Services GovCloud at U-M
- Andrew File System (AFS)
- Armis2
- BlueJeans Videoconferencing
- Box Additional Apps (Non-Core)
- Box at U-M Core Apps
- Canvas
- Cloud Storage Included with Software
- Data Warehouse
- Desktop Backup (Powered by Code42)
- Digital Signage
- Document Imaging System
- Dropbox at U-M
- E-signature Service - SignNow
- Echo360 - Lecture Capture and LectureTools
- Electronic Research Notebook at U-M
- eResearch
- Globus
- Google at U-M Core Services
- Google Cloud Platform at U-M
- Google Drive at U-M
- Google Mail and Calendar at U-M
- Google Non-Core Services
- Gradescope
- Great Lakes Cluster
- ITS Exchange Email and Calendar
- LastPass at Michigan Medicine
- MiBackup
- Michigan Medicine Exchange/Outlook Email and Calendar
- Microsoft Azure at U-M
- Microsoft Office 365 at U-M
- MiDatabase
- MiDesktop
- MiServer
- MiShare
- MiStorage (NFS)
- MiStorage CIFS with AWS S3 Cloud Storage Integration
- MiVideo
- MiWorkspace
- Personal Accounts
- Personally Owned Devices (phone, tablet, laptop, etc.)
- Perusall
- Piazza Q&A
- Qualtrics
- ServiceNow at Michigan Medicine
- Statistics and Computation Service
- TeamDynamix at U-M
- Turbo Research Storage (NFS)
- Turbo Research Storage (NFSv4+Kerberos or CIFS)
- Virtru at U-M
- Yottabyte Research Cloud



The Sensitive Data Guide provides guidance to help make informed decisions about where to safely store and share university data.

It is not intended to be a complete or comprehensive catalog of services available at U-M.

safecomputing.umich.edu/dataguide

Data Classification In Action

Questions to ask:

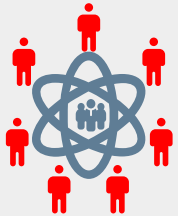
- ➔ What type of data is it?
- ➔ What is the level of sensitivity?
  - Level of harm to individuals
  - Subject to contracts or regulations

safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/examples-by-level

NAVIGATING THE SENSITIVITY LEVELS

Human Subjects Research Data

MODERATE



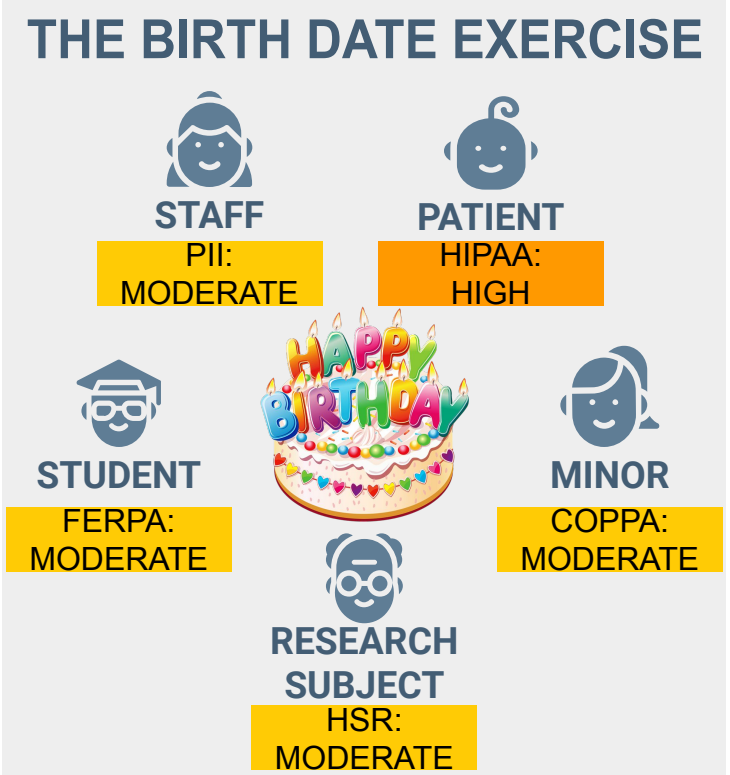
Sensitive Identifiable Human Subjects Research Data

HIGH

Data Classification In Action

Questions to ask:

- ➔ What type of data is it?
- ➔ Who does the data concern?
- ➔ Is it regulated?



Data Classification In Action

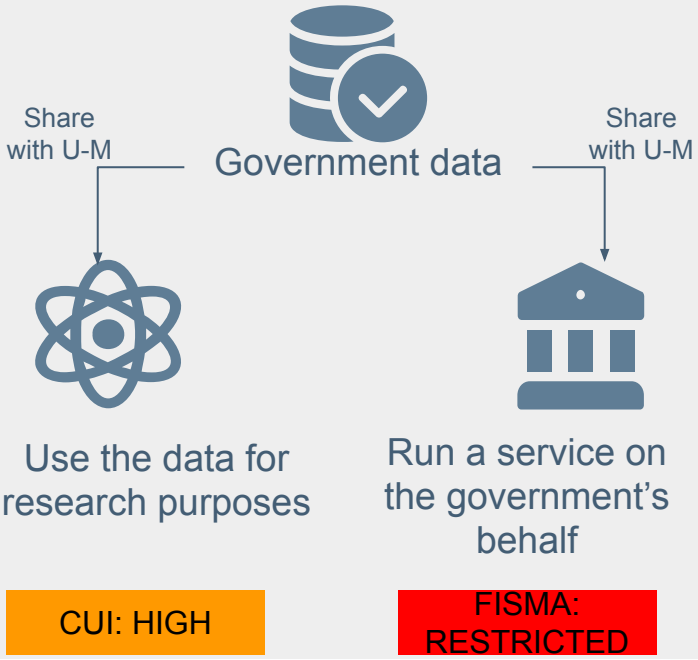
Questions to ask:

- ➔ What type of data is it?
- ➔ What is the purpose of the data?

CUI: Controlled Unclassified Information

FISMA: Federal Information Security Management Act

CUI vs. FISMA EXERCISE



Data Classification In Action

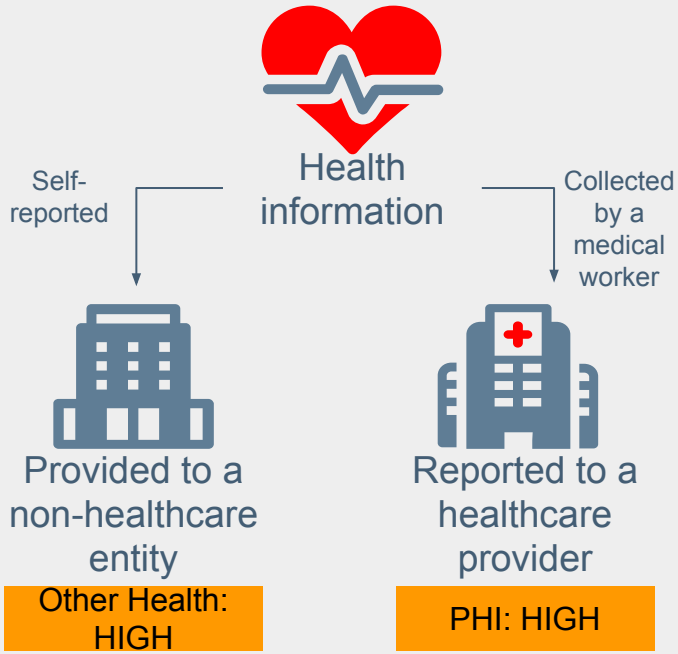
Security is not the same as compliance

Questions to ask:

- ➔ What type of data is it?
- ➔ How is the data collected?
- ➔ To whom is the data provided?

PHI: Protected Health Information (needs BAA)

HEALTH DATA vs. PHI EXERCISE



Protecting Sensitive Data

Sensitive Data must be protected to prevent theft, unauthorized access, compromise, and inappropriate use.

Policies and Standards	Minimum Security Requirements	Vendor Security
Recently revised policy (SPG 601.27) and accompanying information security standards	Organized by information security standard and based on data sensitivity levels	Third Party Vendor Security and Compliance Standard (DS-20) and additional guidance

Policies and Standards

- The U-M Information Security Policy (SPG 601.27) was updated in June 2018.
- It is supported and supplemented by 13 specific operational, procedural, and technical standards.

1. Access, Authorization, and Authentication Management (DS-22)
2. Disaster Recovery Planning and Data Backup for Information Systems and Services (DS-12)
3. Electronic Data Disposal and Media Sanitization (DS-11)
4. Encryption (DS-15)
5. Information Assurance Awareness, Training, and Education (DS-16)
6. Information Security Risk Management (DS-13)
7. Network Security (DS-14)
8. Physical Security (DS-17)
9. Secure Coding and Application Security (DS-18)
10. Security of Enterprise Application Integration (DS-09)
11. Security Log Collection, Analysis, and Retention (DS-19)
12. Third Party Vendor Security and Compliance (DS-20)
13. Vulnerability Management (DS-21)

Security and Compliance at U-M

- Do not conflate security and compliance
- Security and compliance are a shared responsibility
- Alignment vs. compliance: do the right thing to the best of your ability
- Using common sense
- It’s a never-ending journey
- Information Assurance is a partner and a resource to you

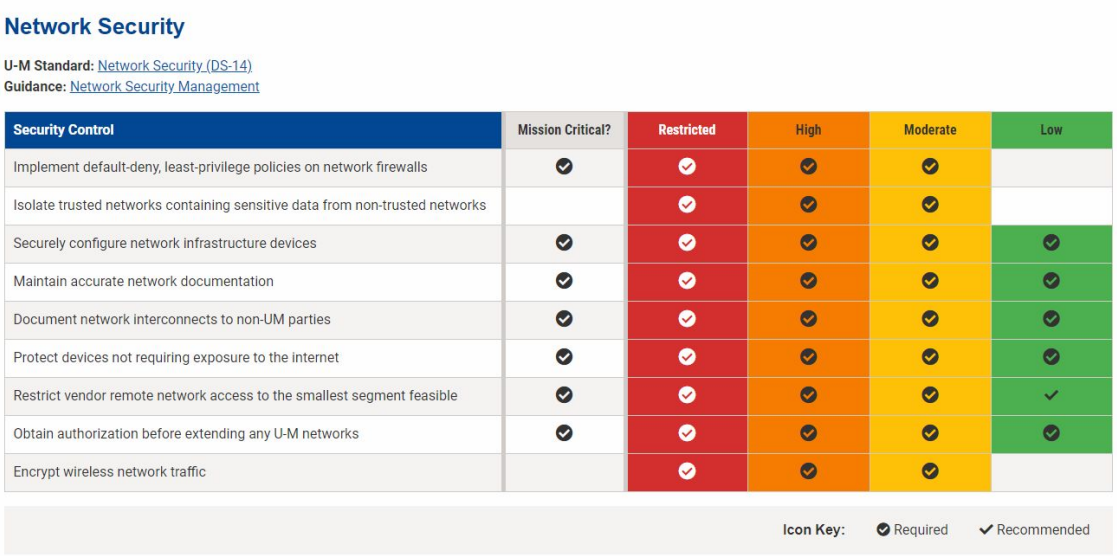
Incremental Improvement Is Still Improvement

DISCUSSION

APPENDIX

Minimum Security Requirements

Available on the [Safe Computing website]



Network Security

U-M Standard: Network Security (DS-14)
Guidance: Network Security Management

Security Control	Mission Critical?	Restricted	High	Moderate	Low
Implement default-deny, least-privilege policies on network firewalls	●	●	●	●	
Isolate trusted networks containing sensitive data from non-trusted networks		●	●	●	
Securely configure network infrastructure devices	●	●	●	●	●
Maintain accurate network documentation	●	●	●	●	●
Document network interconnects to non-UM parties	●	●	●	●	●
Protect devices not requiring exposure to the internet	●	●	●	●	●
Restrict vendor remote network access to the smallest segment feasible	●	●	●	●	✓
Obtain authorization before extending any U-M networks	●	●	●	●	●
Encrypt wireless network traffic		●	●	●	

Icon Key: ● Required ✓ Recommended

Third Party Vendor Security

- Any external service provider that transmits, stores, or processes university data is considered a third party vendor
- Follow the Third Party Vendor Security and Compliance Standard (DS-20)
- Additional Guidance is available on the Safe Computing website

Vendor Assessment Process

1. Engage Procurement Services if possible
2. Determine Data classification (consult with IA if needed)
3. Based on data classification, the following agreements may be needed:
   - → Data Protection Agreement (DPA) or equivalent
   - → FERPA Agreement
   - → Third Party Security Questionnaire (UMSPSCQ/BTAA or equivalent)
   - → Business Associate Agreement (BAA)